Amendments to the claims:

Claims:

1. (Currently Amended) A method for ~~effecting~~ using a secure computing device to secure transactions over a computer network that includes an untrusted client computer with a user interface and a server computer connected to the computer network, in a manner designed to foil identity theft perpetrated from the client computer, comprising:

connecting ~~a~~ the secure computing device to the untrusted client computer and the network;

operating the secure computing device to communicate a list of available services, for which the secure computing device stores private information corresponding to the service, to the client computer;

in response ~~responsive~~ to receiving the list of available services, using the user interface to display the list of available services to a user;

in response ~~responsive~~ to a selection of one available service by the user, establishing a secure connection from the secure computing device to the server;

transmitting from the secure computing device to the server computer user identifying information including a shared secret;

establishing a secure connection from the untrusted client computer to the server computer;

operating the server computer to create a one-to-one mapping between the secure computing device and the untrusted client computer;

receiving an attempted entry of the shared secret by the user from the untrusted client computer;

if the entered shared secret matches the shared secret, permitting the user to interact with a service provided by the server computer~~securely communicating private information from the secure computing device to the server over the secure connection~~.

2. (Previously Presented) The method of Claim 1 further comprising:
authenticating a user based on the private information; and
in response to successful authentication of the user, conducting a transaction between the client computer and the server computer.

3. (Currently Amended) The method of Claim 1 ~~further comprising:~~ wherein the connection between the secure computing device and the untrusted client is a direct connection and wherein the secure computing device is connected to the network via the untrusted client.
~~transmitting from the secure computing device to the server computer user identifying information~~.

4. (Currently Amended) The method of Claim ~~3~~1 wherein the ~~user identifying information includes~~ shared secret is a secret personal identification number (sPIN).

5. (Currently Amended) The method of Claim [4]1 further ~~comprising~~ wherein~~: responsive to receiving~~ the user identifying information includes a unique identifier for the untrusted client computer and wherein the one-to-one mapping is created using the unique identifier~~, operating the server computer to establish an association among the user, the client and the secure computing device~~.

6. (Original) The method of Claim 4 wherein the secure computing device has a personal identification number (PIN) wherein the sPIN and the PIN are unrelated.

7. (Original) The method of Claim 4 wherein the server computer uses the sPIN for only one session.

8. (Original) The method of Claim 4 wherein the portable secure computing device is a smart card.

9. (Currently Amended) A method for secure transactions over a computer network that includes an untrusted client computer with a user interface and a server computer, in a manner designed to foil identity theft perpetrated from the client computer, comprising:

   connecting a secure computing device to the network;

   establishing a secure connection from the secure computing device to the server;

   securely communicating ~~private information~~ a shared secret from the secure computing device to the server over the secure connection;

   establishing a secure connection from the untrusted client computer to the server computer;

operating the server computer to create a one-to-one mapping between the secure computing device and the untrusted client computer;

receiving an attempted entry of the shared secret by the user from the untrusted client computer;

authenticating a user ~~using~~ by comparing the ~~private information~~ attempted entry of the shared secret and the shared secret; and

in response to successfully authenticating the user, conducting a transaction between the untrusted client and the server.

10. (Original) The method of Claim 9 wherein the step of securely communicating private information comprises pushing the private information from the secure computing device to the server computer.

11. (Currently Amended) The method of Claim 10 further comprising:

in response to successfully authenticating a user to the service, operating the client to transmit an indication to the server that the secure computing device will send information necessary for a transaction;

operating the server to wait for the information from the secure computing device;

operating the client to select the information necessary for the transaction; and

in response to selecting the information necessary for the transaction, operating the secure computing device to transmit the selected information securely to the server.

12. (Original) The method of Claim 9 wherein the step of securely communicating private information comprises operating the server computer to pull the private information from the secure computing device.

13. (Original) The method of Claim 9 further comprising:

in response to successfully authenticating a user, operating the server to transmit a request to the secure computing device to provide information necessary to complete a transaction;

in response to a request from the server for information necessary to complete a transaction, operating the secure computing device to notify the client that the server has made the request for information necessary to complete a transaction;

in response to notification from the secure computing device that the server is requesting the information necessary to complete a transaction, operating the client to obtain a user's approval or denial of the request; and

in response to a user's approval, transmitting the requested information from the secure computing device to the server in a secure manner.

14. (Currently Amended) A system for effecting secure transactions over a computer network that includes an untrusted client computer with a user interface and a server computer, in a manner designed to foil identity theft through keystroke logging, comprising:

a secure computing device connected to the computer network and capable of establishing a secure connection with the server computer and the client computer;

wherein the secure computing device has logic operable to store private user information; and

wherein the secure computing device has logic, in response to the initiation of a transaction between a user operating the client computer and the server computer, operable to securely transmit a message containing identifying information linking the secure computing device and the untrusted client computer, and a shared secret ~~the private user information~~ to the server computer in a manner such that only the server can interpret the private user information;

a server comprising logic to

receive the message containing identifying information;

in response to receiving the message containing identifying information creating a one-to-one mapping between the secure computing device and the untrusted computer;

receiving an attempted entry of the shared secret by the user from the untrusted client computer;

if the attempted entry of the shared secret matches the shared secret, permitting the user to interact with a service provided by the server computer.

15. (Currently Amended) The system for effecting secure transactions over a computer network of Claim 14:

wherein the message containing identifying information contains ~~secure computing device has logic to transmit a map to the server computer, the map having~~ the elements clientIP,

cardIP, login credentials, and secret personal identification number (sPIN);

wherein the server computer has logic to request the user to enter the sPIN and logic to verify that the entered sPIN matches the sPIN in the map.

16. (Original) The system for effecting secure transactions over a computer network of Claim 15:

wherein the server computer has logic to destroy the map if the sPIN entered by the user does not match the sPIN of the map.

17. (Previously Presented) The system for effecting secure transactions over a computer network of Claim 14:

wherein the secure computing device transmits the private user information upon a request by the user.

18. (Previously Presented) The system for effecting secure transactions over a computer network of Claim 14:

wherein the secure computing device transmits the private user information upon a request by the server computer.

19. (Previously Presented) The system for effecting secure transactions over a computer network of Claim 18:

wherein the secure computing device transmits the private user information to the server computer only upon permission granted by the user.

20. (Original) The system for effecting secure transactions over a computer network of Claim 19:

wherein the server computer destroys the map in response to invalid sPIN, denial of permission from the user, and transaction completion.

21. (New) The method of Claim 1 further comprising:

operating the server computer to request confidential information from the user;

on the user's request, transmitting from the untrusted client computer to the secure computing device a command to transmit the confidential information from the secure computing device to the server;

in response to the command to transmit the confidential information, transmitting the confidential information from the secure computing device to the server; and

completing a transaction using the confidential information.